11-24-00

A

Practitioner's Docket No. 770P009595-US (PAR) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of

Inventor(s): George M. Brookner
Lorenz R. Frey

WARNING: *37 C.F.R. § 1.41(a)(1) points out:*

"(a) A patent is applied for in the name or names of the actual inventor or inventors.

"(1) The inventorship of a nonprovisional application is that inventorship set forth in the oath or declaration as prescribed by § 1.63, except as provided for in § 1.53(d)(4) and § 1.63(d). If an oath or declaration as prescribed by § 1.63 is not filed during the pendency of a nonprovisional application, the inventorship is that inventorship set forth in the application papers filed pursuant to § 1.53(b), unless a petition under this paragraph accompanied by the fee set forth in § 1.17(i) is filed supplying or changing the name or names of the inventor or inventors."

For (title):
GENERATION AND MANAGEMENT OF CUSTOMER PIN'S

CERTIFICATION UNDER 37 C.F.R. § 1.10*
(Express Mail label number is mandatory.)
(Express Mail certification is optional.)

I hereby certify that this New Application Transmittal and the documents referred to as attached therein are being deposited with the United States Postal Service on this date 11/22/00, in an envelope as "Express Mail Post Office to Addressee," mailing Label Number EL 627 422 030 US, addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

June Adams
(type or print name of person mailing paper)

June Adams
Signature of person mailing paper

WARNING: *Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. § 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.*

***WARNING:** *Each paper or fee filed by "Express Mail" **must** have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. § 1.10(b).*
*"Since the filing of correspondence under § 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will **not** be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.*

1. Type of Application

This new application is for a(n)

(check one applicable item below)

☒ Original (nonprovisional)

□ Design

□ Plant

WARNING: ***Do not*** *use this transmittal for a completion in the U.S. of an International Application under 35 U.S.C. § 371(c)(4), unless the International Application is being filed as a divisional, continuation or continuation-in-part application.*

WARNING: ***Do not*** *use this transmittal for the filing of a provisional application.*

NOTE: *If one of the following 3 items apply, then complete and attach ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF A PRIOR U.S. APPLICATION CLAIMED and a NOTIFICATION IN PARENT APPLICATION OF THE FILING OF THIS CONTINUATION APPLICATION.*

□ Divisional.

□ Continuation.

□ Continuation-in-part (C-I-P).

2. Benefit of Prior U.S. Application(s) (35 U.S.C. §§ 119(e), 120, or 121)

NOTE: *A nonprovisional application may claim an invention disclosed in one or more prior filed copending nonprovisional applications or copending international applications designating the United States of America. In order for a nonprovisional application to claim the benefit of a prior filed copending nonprovisional application or copending international application designating the United States of America, each prior application must name as an inventor at least one inventor named in the later filed nonprovisional application and disclose the named inventor's invention claimed in at least one claim of the later filed nonprovisional application in the manner provided by the first paragraph of 35 U.S.C. § 112. Each prior application must also be:*

(i) An international application entitled to a filing date in accordance with PCT Article 11 and designating the United States of America; or

(ii) Complete as set forth in § 1.51(b); or

(iii) Entitled to a filing date as set forth in § 1.53(b) or § 1.53(d) and include the basic filing fee set forth in § 1.16; or

(iv) Entitled to a filing date as set forth in § 1.53(b) and have paid therein the processing and retention fee set forth in § 1.21(l) within the time period set forth in § 1.53(f).

37 C.F.R. § 1.78(a)(1).

NOTE: *If the new application being transmitted is a divisional, continuation or a continuation-in-part of a parent case, or where the parent case is an International Application which designated the U.S., or benefit of a prior provisional application is claimed, then check the following item and complete and attach ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.*

WARNING: *If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. §§ 120, 121 or 365(c), the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. §§ 120, 121 or 365(c). (35 U.S.C. § 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. §§ 119, 365(a) or 365(b).) For a c-i-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.*

WARNING: *When the last day of pendency of a provisional application falls on a Saturday, Sunday, or Federal holiday within the District of Columbia, any nonprovisional application claiming benefit of the provisional application* ***must*** *be filed prior to the Saturday, Sunday, or Federal holiday within the District of Columbia. See 37 C.F.R. § 1.78(a)(3).*

□ The new application being transmitted claims the benefit of prior U.S. application(s). Enclosed are ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

3. Papers Enclosed

A. Required for filing date under 37 C.F.R. § 1.53(b) (Regular) or 37 C.F.R. § 1.153 (Design) Application

_22_ Pages of specification

_5_ Pages of claims

_3_ Sheets of drawing

WARNING: ***DO NOT*** *submit original drawings. A high quality copy of the drawings should be supplied when filing a patent application. The drawings that are submitted to the Office must be on strong, white, smooth, and non-shiny paper and meet the standards according to § 1.84. If corrections to the drawings are necessary, they should be made to the original drawing and a high-quality copy of the corrected original drawing then submitted to the Office. Only one copy is required or desired. For comments on proposed then-new 37 C.F.R. § 1.84, see Notice of March 9, 1988 (1990 O.G. 57-62).*

NOTE: *"Identifying indicia, if provided, should include the application number or the title of the invention, inventor's name, docket number (if any), and the name and telephone number of a person to call if the Office is unable to match the drawings to the proper application. This information should be placed on the back of each sheet of drawing a minimum distance of 1.5 cm. (5/8 inch) down from the top of the page . . ." 37 C.F.R. § 1.84(c)).*

(complete the following, if applicable)

□ The enclosed drawing(s) are photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)." 37 C.F.R. § 1.84(b).

□ formal

□ informal

B. Other Papers Enclosed

_____ Pages of declaration and power of attorney

_1_ Pages of abstract

_____ Other

4. Additional papers enclosed

□ Amendment to claims

□ Cancel in this applications claims ____________________ before calculating the filing fee. (At least one original independent claim must be retained for filing purposes.)

□ Add the claims shown on the attached amendment. (Claims added have been numbered consecutively following the highest numbered original claims.)

□ Preliminary Amendment

□ Information Disclosure Statement (37 C.F.R. § 1.98)

□ Form PTO–1449 (PTO/SB/08A and 08B)

□ Citations

□ Declaration of Biological Deposit

□ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence.

□ Authorization of Attorney(s) to Accept and Follow Instructions from Representative

□ Special Comments

□ Other

5. Declaration or oath (including power of attorney)

NOTE: *A newly executed declaration is not required in a continuation or divisional application provided that the prior nonprovisional application contained a declaration as required, the application being filed is by all or fewer than all the inventors named in the prior application, there is no new matter in the application being filed, and a copy of the executed declaration filed in the prior application (showing the signature or an indication thereon that it was signed) is submitted. The copy must be accompanied by a statement requesting deletion of the names of person(s) who are not inventors of the application being filed. If the declaration in the prior application was filed under § 1.47, then a copy of that declaration must be filed accompanied by a copy of the decision granting § 1.47 status or, if a nonsigning person under § 1.47 has subsequently joined in a prior application, then a copy of the subsequently executed declaration must be filed. See 37 C.F.R. §§ 1.63(d)(1)-(3).*

NOTE: *A declaration filed to complete an application must be executed, identify the specification to which it is directed, identify each inventor by full name including family name and at least one given name, without abbreviation together with any other given name or initial, and the residence, post office address and country or citizenship of each inventor, and state whether the inventor is a sole or joint inventor. 37 C.F.R. § 1.63(a)(1)-(4).*

□ Enclosed

Executed by

(check **all** *applicable boxes)*

□ inventor(s).

□ legal representative of inventor(s).
37 C.F.R. §§ 1.42 or 1.43.

□ joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.

□ This is the petition required by 37 C.F.R. § 1.47 and the statement required by 37 C.F.R. § 1.47 is also attached. *See* item 13 below for fee.

☒ Not Enclosed.

NOTE: *Where the filing is a completion in the U.S. of an International Application or where the completion of the U.S. application contains subject matter in addition to the International Application, the application may be treated as a continuation or continuation-in-part, as the case may be, utilizing ADDED PAGE FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION CLAIMED.*

☒ Application is made by a person authorized under 37 C.F.R. § 1.41(c) on behalf of *all* the above named inventor(s).

(The declaration or oath, along with the surcharge required by 37 C.F.R. § 1.16(e) can be filed subsequently).

□ Showing that the filing is authorized.
(not required unless called into question. 37 C.F.R. § 1.41(d))

6. Inventorship Statement

WARNING: *If the named inventors are each not the inventors of all the claims an explanation, including the ownership of the various claims at the time the last claimed invention was made, should be submitted.*

The inventorship for all the claims in this application are:

□ The same.

or

□ Not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,

□ is submitted.

□ will be submitted.

7. Language

NOTE: *An application including a signed oath or declaration may be filed in a language other than English. An English translation of the non-English language application and the processing fee of $130.00 required by 37 C.F.R. § 1.17(k) is required to be filed with the application, or within such time as may be set by the Office. 37 C.F.R. § 1.52(d).*

□ English

□ Non-English

□ The attached translation includes a statement that the translation is accurate. 37 C.F.R. § 1.52(d).

8. Assignment

☒ An assignment of the invention to Ascom Hasler Mailing Systems, Inc.

□ is attached. A separate □ "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or □ FORM PTO 1595 is also attached.

☒ will follow.

NOTE: *"If an assignment is submitted with a new application, send two separate letters-one for the application and one for the assignment." Notice of May 4, 1990 (1114 O.G. 77-78).*

WARNING: *A newly executed "CERTIFICATE UNDER 37 C.F.R. § 3.73(b)" must be filed when a continuation-in-part application is filed by an assignee. Notice of April 30, 1993, 1150 O.G. 62-64.*

9. Certified Copy

Certified copy(ies) of application(s)

Country	Appln. No.	Filed
Country	Appln. No.	Filed
Country	Appln. No.	Filed

from which priority is claimed

□ is (are) attached.

□ will follow.

NOTE: *The foreign application forming the basis for the claim for priority must be referred to in the oath or declaration. 37 C.F.R. § 1.55(a) and 1.63.*

NOTE: *This item is for any foreign priority for which the application being filed directly relates. If any parent U.S. application or International Application from which this application claims benefit under 35 U.S.C. § 120 is itself entitled to priority from a prior foreign application, then complete item 18 on the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.*

10. Fee Calculation (37 C.F.R. § 1.16)

A. ☒ Regular application

CLAIMS AS FILED

	Number filed		Number Extra		Rate	Basic Fee 37 C.F.R. 1.16(a) $710.00
Total Claims (37 C.F.R. § 1.16(c))	30	− 20 =	10	×	$ 18.00	180.00
Independent Claims (37 C.F.R. § 1.16(b))	3	− 3 =	0	×	$ 80.00	
Multiple dependent claim(s), if any (37 C.F.R. § 1.16(d))				+	$260.00	

□ Amendment cancelling extra claims is enclosed.

□ Amendment deleting multiple-dependencies is enclosed.

□ Fee for extra claims is not being paid at this time.

NOTE: *If the fees for extra claims are not paid on filing they must be paid or the claims cancelled by amendment, prior to the expiration of the time period set for response by the Patent and Trademark Office in any notice of fee deficiency. 37 C.F.R. § 1.16(d).*

Filing Fee Calculation $890.00

B. □ Design application
($310.00—37 C.F.R. § 1.16(f))

Filing Fee Calculation $________

C. □ Plant application
($480.00—37 C.F.R. § 1.16(g))

Filing fee calculation $________

11. Small Entity Statement(s)

□ Statement(s) that this is a filing by a small entity under 37 C.F.R. § 1.9 and 1.27 is (are) attached.

WARNING: *"Status as a small entity must be specifically established in each application or patent in which the status is available and desired. Status as a small entity in one application or patent does not affect any other application or patent, including applications or patents which are directly or indirectly dependent upon the application or patent in which the status has been established. The refiling of an application under § 1.53 as a continuation, division, or continuation-in-part (including a continued prosecution application under § 1.53(d)), or the filing of a reissue application requires a new determination as to continued entitlement to small entity status for the continuing or reissue application. A nonprovisional application claiming benefit under 35 U.S.C. § 119(e), 120, 121, or 365(c) of a prior application, or a reissue application may rely on a statement filed in the prior application or in the patent if the nonprovisional application or the reissue application includes a reference to the statement in the prior application or in the patent or includes a copy of the statement in the prior application or in the patent and status as a small entity is still proper and desired. The payment of the small entity basic statutory filing fee will be treated as such a reference for purposes of this section." 37 C.F.R. § 1.28(a)(2).*

WARNING: *"Small entity status must not be established when the person or persons signing the . . . statement can **unequivocally** make the required self-certification." M.P.E.P., § 509.03, 6th ed., rev. 2, July 1996 (emphasis added).*

(complete the following, if applicable)

□ Status as a small entity was claimed in prior application
______ / ______________, filed on ______________, from which benefit is being claimed for this application under:

35 U.S.C. § □ 119(e),
□ 120,
□ 121,
□ 365(c),

and which status as a small entity is still proper and desired.

□ A copy of the statement in the prior application is included.

Filing Fee Calculation (50% of **A, B** or **C** above)

$______________________

NOTE: Any excess of the full fee paid will be refunded if small entitiy status is established and a refund request are filed within 2 months of the date of timely payment of a full fee. The two-month period is not extendable under § 1.136. 37 C.F.R. § 1.28(a).

12. Request for International-Type Search (37 C.F.R. § 1.104(d))

(complete, if applicable)

□ Please prepare an international-type search report for this application at the time when national examination on the merits takes place.

13. **Fee Payment Being Made at This Time**

□ Not Enclosed

□ No filing fee is to be paid at this time.
(This and the surcharge required by 37 C.F.R. § 1.16(e) can be paid subsequently.)

☒ Enclosed

☒ Filing fee	$ 890.00
□ Recording assignment ($40.00; 37 C.F.R. § 1.21(h)) (See attached "COVER SHEET FOR ASSIGNMENT ACCOMPANYING NEW APPLICATION".)	$
□ Petition fee for filing by other than all the inventors or person on behalf of the inventor where inventor refused to sign or cannot be reached ($130.00; 37 C.F.R. §§ 1.47 and 1.17(i))	$
□ For processing an application with a specification in a non-English language ($130.00; 37 C.F.R. §§ 1.52(d) and 1.17(k))	$
□ Processing and retention fee ($130.00; 37 C.F.R. §§ 1.53(d) and 1.21(l))	$
□ Fee for international-type search report ($40.00; 37 C.F.R. § 1.21(e))	$

NOTE: 37 C.F.R. § 1.21(l) establishes a fee for processing and retaining any application that is abandoned for failing to complete the application pursuant to 37 C.F.R. § 1.53(f) and this, as well as the changes to 37 C.F.R. §§ 1.53 and 1.78(a)(1), indicate that in order to obtain the benefit of a prior U.S. application, either the basic filing fee must be paid, or the processing and retention fee of § 1.21(l) must be paid, within 1 year from notification under § 53(f).

Total fees enclosed $ 890.00

14. **Method of Payment of Fees**

☒ Check in the amount of $ 890.00

□ Charge Account No. ______________ in the amount of $______.
A duplicate of this transmittal is attached.

NOTE: Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 C.F.R. § 1.22(b).

15. Authorization to Charge Additional Fees

WARNING: *If no fees are to be paid on filing, the following items should not be completed.*

WARNING: *Accurately count claims, especially multiple dependent claims, to avoid unexpected high charges, if extra claim charges are authorized.*

☒ The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. 16-1350 :

☒ 37 C.F.R. § 1.16(a), (f) or (g) (filing fees)

☒ 37 C.F.R. § 1.16(b), (c) and (d) (presentation of extra claims)

NOTE: Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 C.F.R. § 1.16(d)), it might be best not to authorize the PTO to charge additional claim fees, except possibly when dealing with amendments after final action.

☒ 37 C.F.R. § 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

☒ 37 C.F.R. § 1.17(a)(1)-(5) (extension fees pursuant to § 1.136(a)).

☒ 37 C.F.R. § 1.17 (application processing fees)

NOTE: ". . .A written request may be submitted in an application that is an authorization to treat any concurrent or future reply, requiring a petition for an extension of time under this paragraph for its timely submission, as incorporating a petition for extension of time for the appropriate length of time. An authorization to charge all required fees, fees under § 1.17, or all required extension of time fees will be treated as a constructive petition for an extension of time in any concurrent or future reply requiring a petition for an extension of time under this paragraph for its timely submission. Submission of the fee set forth in § 1.17(a) will also be treated as a constructive petition for an extension of time in any concurrent reply requiring a petition for an extension of time under this paragraph for its timely submission." 37 C.F.R. § 1.136(a)(3).

□ 37 C.F.R. § 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. § 1.311(b))

NOTE: Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 C.F.R. § 1.311(b).

NOTE: 37 C.F.R. § 1.28(b) requires "Notification of any change in status resulting in loss of entitlement to small entity status must be filed in the application . . . prior to paying, or at the time of paying, . . . the issue fee. . . " From the wording of 37 C.F.R. § 1.28(b), (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.

16. Instructions as to Overpayment

NOTE: *". . . Amounts of twenty-five dollars or less will not be returned unless specifically requested within a reasonable time, nor will the payer be notified of such amounts; amounts over twenty-five dollars may be returned by check or, if requested, by credit to a deposit account."* 37 *C.F.R.* § *1.26(a).*

☒ Credit Account No. 16-1350

□ Refund

David Aker

SIGNATURE OF PRACTITIONER

Reg. No. 29,277

David Aker

(type or print name of attorney)

Tel. No. (203) 259-1800

Perman & Green, LLP

P.O. Address

Customer No. 2512

425 Post Road
Fairfield, CT 06430

☒ **Incorporation by reference of added pages**

(check the following item if the application in this transmittal claims the benefit of prior U.S. application(s) (including an international application entering the U.S. stage as a continuation, divisional or C-I-P application) and complete and attach the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED)

☒ Plus Added Pages for New Application Transmittal Where Benefit of Prior U.S. Application(s) Claimed

Number of pages added 5

□ Plus Added Pages for Papers Referred to in Item 4 Above

Number of pages added ______

□ Plus added pages deleting names of inventor(s) named in prior application(s) who is/are no longer inventor(s) of the subject matter claimed in this application.

Number of pages added ______

□ Plus "Assignment Cover Letter Accompanying New Application"

Number of pages added ______

□ **Statement Where No Further Pages Added**

(if no further pages form a part of this Transmittal, then end this Transmittal with this page and check the following item)

□ This transmittal ends with this page.

Practitioner's Docket No. 770P009595-US (PAR) **PATENT**

ADDED PAGES FOR APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED

NOTE: See 37 CFR 1.78(a).

17. Relate Back

WARNING: If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. 120, 121 or 365(c), the 20–year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. 120, 121 or 365(c). (35 U.S.C. 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. 119, 365(a) or 365(b).) For a c–i–p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.

(complete the following, if applicable)

□ Amend the specification by inserting, before the first line, the following sentence:

A. 35 U.S.C. 119(e)

NOTE: "Any nonprovisional application claiming the benefit of one or more prior filed copending provisional applications must contain or be amended to contain in the first sentence of the specification following the title a reference to each such prior provisional application, identifying it as a provisional application, and including the provisional application number (consisting of series code and serial number)." 37 C.F.R. § 1.78(a)(4).

☒ "This application claims the benefit of U.S. Provisional Application(s) No(s).:

APPLICATION NO(S).:	FILING DATE
60 / 166,734	11/22/99 "
/	"
/	"

B. 35 U.S.C. 120, 121 and 365(c)

NOTE: *"Any nonprovisional application claiming the benefit of one or more prior filed copending nonprovisional applications or international applications designating the United States of America must contain or be amended to contain in the first sentence of the specification following the title a reference to each such prior application, identifying it by application number (consisting of the series code and serial number) or international application number and international filing date and indicating the relationship of the applications. Cross-references to other related applications may be made when appropriate." (See § 1.14(b)). 37 C.F.R. § 1.78(a)(2).*

□ "This application is a

- □ continuation
- □ continuation-in-part
- □ divisional

of copending application(s)

□ application number 0 /____________________ filed on ____________"

□ International Application ____________________ filed on

____________________ and which designated the U.S."

NOTE: *The proper reference to a prior filed PCT application that entered the U.S. national phase is the U.S. serial number and the filing date of the PCT application that designated the U.S.*

NOTE: *(1) Where the application being transmitted adds subject matter to the International Application, then the filing can be as a continuation-in-part or (2) if it is desired to do so for other reasons then the filing can be as a continuation.*

□ "The nonprovisional application designated above, namely application ______ / ____________________, filed __________, claims the benefit of U.S. Provisional Application(s) No(s).:

APPLICATION NO(S).:	**FILING DATE**
______ /____________________	______________"
______ /____________________	______________"
______ /____________________	______________"

NOTE: *The deadline for entering the national phase in the U.S. for an international application was clarified in the Notice of April 28, 1987 (1079 O.G. 32 to 46) as follows:*

> *"The Patent and Trademark Office considers the International application to be pending until the 22nd month from the priority cate if the United States has been designated and no Demand for International Preliminary Examination has been filed prior to the expiration of the 19th month from the priority date and until the 32nd month from the priority date if a Demand for International Preliminary Examination which elected the United States of America has been filed prior to the expiration of the 19th month from the priority date, provided that a copy of the international application has been communicated to the Patent and Trademark Office within the 20 or 30 month period respectively. If a copy of the international application has not ceen communicated to the Patent and Trademark Office within the 20 or 30 month period respectively, the international application becomes abandoned as to the United States 20 or 30 months from the priority date respectivley. These periods have been placed in the rules as paragraph (h) of § 1.494 and paragraph (i) of § 1.495. A continuing application under 35 U.S.C. 365(c) and 120 may be filed anytime during the pendency of the international application."*

18. Relate Back—35 U.S.C. 119 Priority Claim for Prior Application

The prior U.S. application(s), including any prior International Application designating the U.S., identified above in item 17B, in turn itself claim(s) foreign priority(ies) as follows:

Country	Appln. no.	Filed on

The certified copy(ies) has (have)

□ been filed on __________, in prior application 0 /______________, which was filed on ______________.

□ is (are) attached.

WARNING: The certified copy of the priority application that may have been communicated to the PTO by the International Bureau may not be relied on without any need to file a certified copy of the priority application ***in the continuing application.*** *This is so because the certified copy of the priority application communicated by the International Bureau is placed in a folder and is not assigned a U.S. serial number unless the national stage is entered. Such folders are disposed of if the national stage is not entered. Therefore, such certified copies may not be available if needed later in the prosecution of a continuing application. An alternative would be to physically remove the priority documents from the folders and transfer them to the continuing application. The resources required to request transfer, retrieve the folders, make suitable record notations, transfer the certified copies, enter and make a record of such copies in the Continuing Application are substantial. Accordingly, the priority documents in folders of international applications that have not entered the national stage may not be relied on. Notice of April 28, 1987 (1079 O.G. 32 to 46).*

19. Maintenance of Copendency of Prior Application

NOTE: The PTO finds it useful if a copy of the petition filed in the prior application extending the term for response is filed with the papers constituting the filing of the continuation application. Notice of November 5, 1985 (1060 O.G. 27).

A. □ Extension of time in prior application

(This item ***must*** *be completed and the papers filed* ***in the prior application,*** *if the period set in the prior application has run.)*

□ A petition, fee and response extends the term in the pending **prior** application until ______________________.

□ A **copy** of the petition filed in prior application is attached.

B. □ Conditional Petition for Extension of Time in Prior Application

(complete this item, if previous item not applicable)

□ A conditional petition for extension of time is being filed in the pending **prior** application.

□ A **copy** of the conditional petition filed in the prior application is attached.

20. Further Inventorship Statement Where Benefit of Prior Application(s) Claimed

NOTE: *"If the continuation, continuation-in-part, or divisional application is filed by less than all the inventors named in the prior application a statement **must** accompany the application when filed requesting deletion of the names of the person or persons who are not inventors of the invention being claimed in the continuation, continuation-in-part, or divisional application." 37 CFR 1.62(a) [emphasis added] (dealing with the file wrapper continuation situation).*

NOTE: *"In the case of a continuation-in-part application which adds and claims additional disclosure by amendment, an oath or declaration as required by § 1.63 must be filed. In those situations where a new oath or declaration is required due to additional subject matter being claimed, additional inventors may be named in the continuing application. In a continuation or divisional application which discloses and claims only subject matter disclosed in a prior application, no additional oath or declaration is required and the application must name as inventors the same or less than all the inventors in the prior application." 37 CFR 1.62(c) (dealing with the continuation situation).*

(complete applicable item (a), (b) and/or (c) below)

(a) □ This application discloses and claims only subject matter disclosed in the prior application whose particulars are set out above and the inventor(s) in this application are

□ the same.

□ less than those named in the prior application. It is requested that the following inventor(s) identified for the prior application be deleted:

____

(type name(s) of inventor(s) to be deleted)

(b) □ This application discloses and claims additional disclosure by amendment and a new declaration or oath is being filed. With respect to the prior application, the inventor(s) in this application are

□ the same.

□ the following additional inventor(s) have been added:

____

(type name(s) of inventor(s) to be added)

(c) The inventorship for all the claims in this application are

□ the same.

□ not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made

□ is submitted.

□ will be submitted.

21. Abandonment of Prior Application *(if applicable)*

□ Please abandon the prior application at a time while the prior application is pending, or when the petition for extension of time or to revive in that application is granted, and when this application is granted a filing date, so as to make this application copending with said prior application.

NOTE: *According to the Notice of May 13, 1983 (103, TMOG 6-7), the filing of a continuation or continuation-in-part application is a proper response with respect to a petition for extension of time or a petition to revive and should include the express abandonment of the prior application conditioned upon the granting of the petition and the granting of a filing date to the continuing application.*

22. Petition for Suspension of Prosecution for the Time Necessary to File an Amendment

WARNING: *"The claims of a new application may be finally rejected in the first Office action in those situations where (1) the new application is a continuing application of, or a substitute for, an earlier application, and (2) all the claims of the new application (a) are drawn to the same invention claimed in the earlier application, and (b) would have been properly finally rejected on the grounds of art of record in the next Office action if they had been entered in the earlier application." MPEP, § 706.07(b).*

NOTE: *Where it is possible that the claims on file will give rise to a first action final for this continuation application and for some reason an amendment cannot be filed promptly (e.g., experimental data is being gathered) it may be desirable to file a petition for suspension of prosecution for the time necessary.*

(check the next item, if applicable)

□ There is provided herewith a Petition To Suspend Prosecution for the Time Necessary to File An Amendment (New Application Filed Concurrently)

23. Small Entity (37 CFR § 1.28(a))

□ Applicant has established small entity status by the filing of a verified statement in parent application ____/________ on ________.

□ A copy of the verified statement previously filed is included.

WARNING: *See 37 CFR § 1.28(a).*

24. NOTIFICATION IN PARENT APPLICATION OF THIS FILING

□ A notification of the filing of this
(check one of the following)

□ continuation

□ continuation-in-part

□ divisional

is being filed in the parent application, from which this application claims priority under 35 U.S.C. § 120.

770P009595-US(PAR)

Patent Application Papers Of:

George M. Brookner

Lorenz R. Frey

For: GENERATION AND MANAGEMENT OF CUSTOMER PIN's

GENERATION AND MANAGEMENT OF CUSTOMER PIN'S

This application claims priority of provisional patent application serial number 60/166,734 filed on November 22, 1999.

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to the generation and management of Personal Identification Numbers (PIN's). More particularly, it relates to the generation and management of PIN's for use in various applications; and more specifically still, in postage franking devices.

Background Art

There are many business and personal financial transactions that must be conducted securely. It is very common for a Personal Identification Number, or PIN to be used to enhance the security of these transactions.

While the use of PIN's generally proceeds smoothly, there are occasional problems. If a PIN holder or customer writes down a PIN, it is subject to discovery by unauthorized users. If it is not written down, the customer may forget the PIN. This requires contacting the financial institution or company having the PIN in its database, and utilizing a PIN reset procedure. It is often necessary for the customer to travel to the location of the company, present identification which must be verified, and then select a new PIN.

SUMMARY OF THE INVENTION

It is an object of the invention to provide a secure method for generating PIN's.

It is another object of the invention to provide an apparatus for securely holding a PIN to help safeguard funds on deposit.

It is yet another object of the invention to provide a convenient way to reset a PIN if a customer loses the PIN.

In accordance with the invention a method for securely generating a PIN comprises generating a number of random binary bits; determining the least significant bits of the number of bits; converting the least significant bits to a decimal integer; shifting the value of the integer by a predetermined constant to produce a shifted integer; and encoding the shifted integer as bits in a PIN block in accordance with a standard, for example the ISO 9564-1 standard.

The number of random bits may be sixty-four. The number of least significant bits may be sixteen. The constant may be 173845. The PIN block may include a control field; a PIN length designation field; a series of PIN digit fields; at least one PIN/transaction digit; and a series of transaction digit fields. Each PIN digit field may represent a binary number having a decimal value of from zero to nine. The control field may be the binary number 0001. The PIN length field may contain a binary number having a decimal value of four, five or six. Thus, at least one PIN/transaction digit is determined in accordance with PIN length. The transaction digit fields may each be four bit binary fields representing a decimal digit of zero to nine. The generation of the number of random binary bits may be accomplished by using a pseudo random number generator.

The invention is also directed to a method for managing security of a PIN used to provide access to a secure device comprising choosing the PIN; storing an encrypted version of the PIN in the device; and communicating the PIN to a user of the device via a communication channel separate and apart from a channel used to provide the device to the user. Preferably, the communication channel is a secure channel, which may be rendered secure by using encryption.

In one embodiment the user of the device chooses the PIN. The manufacturer of the device may cause the encrypted version of the PIN to be stored in the device. The manufacturer may retain a record of the PIN or may discard all records of the PIN.

The PIN may be chosen using a random process, including the one set forth above.

In accordance with the preferred embodiment the device is a postal security device, which stores the value of funds.

The invention also encompasses a method for resetting a PIN in a secure device comprising sending a message to a data center having an original PIN for the device, the message including authorization data indicative of at least one of the device and an authorized user of the device, and securely communicating the original PIN to the location of the device. Preferably, the device has a current PIN, which is replaced with the original PIN. The communicating of the original PIN may comprise sending the original PIN to the user of the device; and the user of the device entering the original PIN into the device. Communication is preferably performed using secure communication. The channels may be rendered secure using secure communications techniques, such as encryption.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing aspects and other features of the present invention are explained in the following description, taken in connection with the accompanying drawings, wherein:

Fig. 1 is a block diagram of a funds storage device connected to a management system server, both in accordance with the invention.

Fig. 2 is a flow diagram illustrating the generation of a PIN in accordance with the invention.

Fig. 3 is a diagram of a PIN block in accordance with the invention.

Fig. 4 is a chart illustrating PIN states and values in accordance with the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention may be used in a broad range of applications. However, for purposes of illustration, it will be described with reference to an apparatus for electronically holding value corresponding to funds, and in particular funds used for generating postage to be applied to items to be mailed. Such a device is often called a Postal Security Device (PSD), or a SAFE™ when produced by Ascom Hasler Mailing Systems.

Referring to Fig. 1, a PSD 10 in accordance with the invention has various hardware and software (or firmware) components. The hardware components include a housing and an electrical connector for connection to PSD 10, (both not represented in Fig. 1). Internal components include an initial PIN register 12 for storing an encoded initial PIN value, for the lifetime of the product. A current PIN register 14 stores an encoded currently valid PIN. A counter 16 counts the number of false PIN entries (FPE). Another counter 18 counts the number of PIN reset operations (PRO). A temporary storage register 20 permits storage of old (still valid) PIN at 20A and a new PIN number at 20B to enable roll-back.

Software components or modules in PSD 20 include a random bit generator 24 and a transaction decryption module 26 to enable decryption of transaction data. The transaction data is typically decrypted by running a 2-key triple-DES (Data Encryption Standard) of a type well known in the art. A separate encoding/decoding function 28 is used for the encoding and decoding of customer PIN data. A roll-back capability 30 is available for PIN modification and/or PIN reset procedures, as more fully described below. An error code and message generator 32 is available to allow a user of the PSD to read error codes which indicate possible system errors, and messages as also more fully described below. An additional communication path 38 is provided from database 36 to PSD 10, and is used as also more fully described below.

As more fully described below with respect to Fig. 2, PSD 10 generates an initial PIN which is transmitted to a server 34 at the manufacturer of PSD 10. Server 34 includes a key management system, not described herein. It also includes a database 36, for storing the value of the PIN, as also more fully described below.

Referring to Fig. 2, the generation of a PSD specific initial PIN takes place during PSD initialization, generally at the manufacturer of the PSD. Using the present random bit generator 24 which may operate in accordance with the ANSI X9.17 standard, a number of random bits, generally sixty-four in number, are generated at 40. All but the least significant bits, preferably sixteen, are discarded at a bit reduction step 42. At step 44 the binary data of the remaining bits from step 42 are converted from binary to decimal form. Since the encryption step generates random bits, the integers resulting from the truncation are uniformly distributed in the interval of 0 to 65,523 for the selection of sixteen bits. Thus, the cryptographic strength of the initial PIN is 16 bits.

At step 46 a shift operation is conducted to guarantee that the initial PIN's resulting from the conversion step are all six digit integers with a lending digit that is not equal to zero. Thus, what are intermediate integer values from step 44, are all shifted to the right by an arbitrarily chosen integer constant. For sixteen bits, this constant may be chosen as 173,845. After this shift, the initial PIN's are uniformly distributed in the interval 173,845 to 239,380.

At step 48 the initial PIN defined at step 46 is encoded according to a standard. PIN encoding following the encoding rules for the IS0/IEC ISO 9564-1 standard are illustrated in Fig. 3.

In Fig. 3, a PIN block 50 which is sixty-four bits in length includes numerous fields. A four bit control field 52 occupies bits 1-4 and is assigned a value of 0001. A pin length field 54, which occupies bits 5-8, contains a four bit binary number with permissible values of binary 0100 to binary 0110 (decimal 4-6). Four PIN digit field 56, 58, 60 and 62 occupy digits 9-12, 13-16, 17-20, and 21-24, respectively. These four 4-bit fields generally have permissible values of binary 0000 to 1001 (decimal zero to nine). However, as previously mentioned, due to the shift to the right (step 46 of Fig. 2) field 56 can never have a value of zero.

Fields 64 and 66 which occupy digits 25-28 and 29-32, respectively are used as either PIN digit fields or transaction digit fields, depending on the length of the PIN. For a six digit PIN, fields 64 and 66 are PIN digit fields. For a five digit PIN, field 64 is a PIN digit field and field 66 may be used as transaction digit field. For a four digit PIN, both of fields 64 and 66 may be used as a transaction digit field. Fields 68, 70, 72, 74, 76, 78, 80 and 82, which occupy block digits 33-36, 37-40, 41-44, 45-48, 49-52, 53-56, 57-60 and 61-64, respectively are all transaction digits, all of which may be 0000. Fields 52, 54 and all transaction digit fields designated as T add redundancy to the PIN value and help to guarantee the uniqueness and integrity of the PIN. There is no difficulty in padding the 64 bit block with zero, because the length of the PIN is encoded in field

54, and is well defined, and it is known that the PIN block always has a length of exactly sixty-four bits.

In operation, the PSD 10 is connected to the customer host system, typically a mail franking system, and is used in a manner well known in the art. The host system has appropriate software for accessing and running PSD 10. Functions that are performed by the host system include encoding of PIN values, encryption of PIN data by running two key triple Data Encryption Standard (DES) and erasure of all PIN data temporarily stored during the customer PIN related operations.

The customer is authenticated using a PIN based mechanism. The PIN is set to a PSD individual initial value in the initialization phase. This value is made known to the customer using a communication path (path 38 of Fig. 1) which is different from the path used for shipping of the PSD itself. The customer is expected to change the PIN when using the PSD the first time. Typical common sense security rules, such as not using birthdays or a sequence of keyboard numbers or letters, changing the PIN periodically, etc. should be used by customers in selecting a new PIN.

The PSD is configured to require the PIN to be entered each time after powering up. The PSD also requires the PIN authentication procedure to be performed again each time the synchronization at the serial interface between the PSD and the host system gets lost. This event indicates to the PSD that it might have been moved to a different host system.

PIN authentication must be performed before any indicia application function is allowed by the PSD (indicia generation and TMS activities). In other words, before doing any franking of mail, or receiving funds from a telemetering system, the PIN must be authenticated.

Whenever a specific consecutive number of authentication failures has occurred (as counted in counter 16 of Fig. 1) the PIN authentication function is locked, which effectively prevents the access to the indicia generation. However, the manufacturer of the PSD may reset the PIN at any time, or provide instructions to the customer as to how to reset the PIN, or cause the PIN to autoreset after a predetermined dormant period.

In order to ensure the effectiveness of the PIN based customer authentication, the PIN shall in general be entered by the customer manually into the host system, which transfers the PIN to the PSD. However, operational needs may require the PIN to be stored externally, e.g. in the host system, and used in an automatic authentication procedure (e.g. prepared scripts). This may be done only if the customer has ensured that the PSD and the host system is protected against theft and misuse by appropriate physical, organizational and/or other technical means.

A session based encryption key established after power up is used to encrypt the PIN before it enters the PSD. Thus, a great advantage of the present invention is that the original PIN, in a clear readable format, is never stored in the PSD, nor transmitted from the PSD.

In the discussion that follows of PIN verification, PIN modification and PIN reset procedures the notation and symbols set forth below are used.

PIN_{init} denotes the initial PIN.

PIN_{cust} denotes the valid Customer PIN.

PIN_{ref} (Reference PIN) denotes the PIN value used by the PSD for customer authentication.

PIN_{tr} (Transaction PIN) denotes the PIN value entered by the customer (e.g. via keyboard in the customer host system).

PIN_{new} (new Customer PIN) denotes a new PIN value chosen by the customer and entered as a replacement for the old value.

PIN'_{xxx} denotes 64-bit PIN block corresponding to PIN_{xxx} as discussed above with respect to Fig. 3.

The symbol $||$ denotes the concatenation of data elements.

The symbol $\oplus$ denotes the bit-wise XOR operation.

In the PIN verification procedure, the following general assumptions apply:

The customer knows the currently valid PIN (PIN_{cust}).

At the beginning of the procedure the PSD keeps the currently valid, encoded PIN (PIN'_{cust}).

The PIN verification procedure, processes and data flows are illustrated below:

Customer ***Host*** ***PSD***

Process 0

Start of PIN verification procedure

<---------------------------------->

Process 1

1) Generates 64 random bits S

------------------------>

$M_0 = S$

Process 2

1) Sets $PIN'_{ref} := PIN'_{cust}$

2) Generates 128 random bits R

<------------------------

$M_1 = R$

Process 3

1) Prompts Customer for PIN entry

Process 4

1) Customer enters PIN_{tr}

------------------------>

$M_2 = PIN_{tr}$

Process 5

1) Encodes PIN_{tr} to form a 64-bit block PIN'_{tr}

2) Sets $K^* := (PIN'_{tr} \,||\, S) \oplus (Const \oplus R)$

3) Parity adjustment of K* to get key K

4) Encrypts PIN'_{tr} (2-key triple-DES) using K

5) Wipes out all traces of PIN_{tr}

------------------------>

$M_3 = Enc(K, PIN'_{tr})$

Process 6

If FPE>FPE$_{max}$ device gets locked

1) Increments FPE (false PIN entry counter)

2) Sets $K^* := (PIN'_{ref} \,||\, S) \oplus (Const \oplus R)$

3) Parity adjustment of K* to get key K

4) Decrypts M_3 using K to get PIN'_{tr}

5) Compares result with PIN'$_{ref}$
If nok Restarts Process 2
else
6) Resets FPE to initial value

<------------------------
ok

------------------------------- **End of *PIN Verification* Procedure** ------------------------

As discussed above, the following message formats may be generated by the PSD, to provide information to the user of the customer host system:

Message M_0

$M_0 := S$

S:		64 bits, random binary data

Message M_1

$M_1 := R$

R	:	128 bits, random binary data

Message M_2

$M_2 := PIN'_{tr}$

PIN'$_{tr}$	:	4-6 digit decimal number

Message M_3

$M_3 := Enc(K, PIN'_{tr})$

M_3	:	64 bits, random binary data
K	:	2-key triple-DES key
PIN'$_{tr}$	:	64 bits, specially encoded data (cf. Annex A)

Process details of step 5 of the PIN verification procedure set forth above in Process 5 are set forth below.

Step 2: **Const** is a 128 bit hard-coded random constant:

(e.g. Const(hex.)=0x 8B44F7AF 895CD7BE FFFF5BB1 49B40821).

Step 4: 2-key triple-DES is run in CBC-mode with IV(hex.)=0x 242070DB 49B40821.

As part of process 6, the customer must be informed in a clear and unequivocal way about the remaining number of PIN entry trials before the PSD gets locked and the possibility to wait for a predefined time period after which the FPE is reset.

A PIN modification procedure is used because the initial PIN values set during the initialization of the PSD, and thought mainly as transport protection, should be changed with this procedure before the device becomes operational. However, in general, this is not enforced technically but only recommended to the customer in an appropriate way. The PIN modification procedure assumes that:

1. The customer knows the currently valid PIN (PIN_{cust});

2. At the beginning of the procedure the PSD keeps the currently valid, encoded PIN (PIN'_{cust});

3. During the procedure the PSD must temporary handle, at the same time, the old PIN value and its replacement in order to enable a roll-back of the procedure; and

4. After the procedure has been successfully executed the PSD stores the encoded new Customer PIN, while the old value is deleted.

As an additional security feature of the PIN modification procedure, there is an integrity check of the new PIN value. The value must be entered twice to assure accuracy before it is accepted. The PIN modification procedure, processes and data flows are set forth below.

Customer ***Host*** ***PSD***

Process 0

Start of PIN modification procedure

<---------------------------------->

Process 1

1) Generates 64 random bits S

----------------------->

$M_0 = S$

Process 2

1) Sets $PIN'_{ref} := PIN'_{cust}$

$M_1 = R$ 2) Generates 64 random bits R

<-----------------------

Process 3

1) Prompts Customer for entry of old and new PIN

Process 4

1) Customer enters PIN_{tr} and PIN_{new} (twice!)

-------------------------->

$M_2 = PIN_{tr}, PIN_{new}, PIN^*_{new}$

Process 5

1) Compares two values PIN_{new} and PIN^*_{new}

If not equal Restarts Process 3

else Verifies correct format of PIN_{new}

If nok Restarts Process 3

else

2) Encodes PIN_{tr} to form a 64-bit block PIN'_{tr}

3) Encodes PIN_{new} to form a 64-bit block PIN'_{new}

4) Sets $K^* := (PIN'_{tr} \,||\, S) \oplus (Const \oplus R)$

5) Parity adjustment of K* to get key K

6) Encrypts PIN'_{new} (2-key triple-DES) using K

7) Wipes out all traces of PIN_{tr} and PIN_{new}

------------------------------>

$M_3 = Enc(K, PIN'_{new})$

Process 6

If $FPE > FPE_{max}$ device gets locked

1) Increments FPE (false PIN entry counter)

2) Sets $K^* := (PIN'_{ref} \,||\, S) \oplus$

$(Const \oplus R)$

3) Parity adjustment of K* to get key K

4) Decrypts M_3 using K to get PIN'$_{new}$

5) Checks correct format of result

If nok Restarts Process 2
else
6) Resets FPE to initial value
7) Sets: PIN'$_{cust}$ = PIN'$_{new}$ (erases old value!)

ok
<----------------------

-------------------------------- **End of *PIN Modification* Procedure** ------------------------

The following error conditions are defined:

0: no error

1: Two values PIN_{new} and $PIN*_{new}$ are different (process 5, step 1)

2: PIN_{new} does not have the correct format (process 5, step 1) The PIN does not satisfy the length requirements and/or begins with a zero and/or consists of all equal digits.

3: PIN verification failed because $PIN'_{ref} \neq PIN'_{tr}$ (process 6, step 5)

For the PIN modification procedure the following message formats apply:

Message M_0

$M_0 := S$

S: 64 bits, random binary data

Message M_1

$M_1 := R$

R : 128 bits, random binary data

Message M_2

$M_2 := PIN_{tr}, PIN_{new}, PIN*_{new}$

PIN_{tr}	:	4-6 digit number
PIN_{new}	:	4-6 digit number
PIN^*_{new}	:	4-6 digit number

Message M_3

$M_3 := Enc(K, PIN'_{new})$

M_3	:	64 bits, random binary data
K	:	2-key triple-DES key
PIN'_{new}	:	64 bits, specially encoded data (cf. Annex A)

Process details for process 5, are the same as set forth above.

As part of process 6, the customer must be informed in a clear and unequivocal way about the remaining number of PIN entry trials before the PSD is locked and the possibility of waiting for a predefined time period after which the FPE (Fig. 1) is reset.

In step 5 checking the correct format here means a verification, that the result of the decryption is a valid PIN block.

Since PIN'_{ref} is part of the encryption key K in the PSD, the chance that a valid PIN block results from the decryption of M_3 is negligibly small ($< 10^{-10}$) if a false value for the Customer PIN (PIN_{tr}) was used as part of the encryption key K in the host. This is due to the large amount of added redundancy contained in a valid PIN block, as described above.

Generally, it is a matter of contractual agreement between the manufacturer and its customers as to under what circumstances a PIN reset procedure is allowed.

Generally, the manufacturer does not have any control over what happens to the customer PIN and how carefully the host is set up, and therefore can take no responsibility for the customer PIN.

The reset procedure described below is therefore intentionally kept simple because the basic security assumption is, that the customer is fully responsible for the correct handling of the PIN. That is, a reset of the PIN should actually never be necessary under normal conditions.

The PIN reset procedure is based on the following general assumptions:

1. The PIN reset procedure consists of a preparatory, intermediate and the final step.

2. The customer does not know the currently valid PIN (PIN_{cust}).

3. At the beginning of the procedure the PSD stores the currently valid, encoded PIN (PIN'_{cust}) and the encoded initial PIN (PIN'_{init}) value set during the PSD initialization phase.

4. During the final step the PSD must temporary handle, at the same time, the old PIN value and its replacement in order to enable a roll-back of the procedure.

5. After the reset procedure has been successfully executed the PSD stores the encoded new Customer PIN value, while the old value is deleted.

6. The encoded initial PIN (PIN'_{init}) value stored in the PSD is not affected (changed, deleted, overwritten) by the procedure.

A manual PIN reset procedure is also provided. In a first step the customer contacts the manufacturer's remote control facility and informs the manufacturer of the situation. This may happen using different communication means such as fax, email, phone etc. This step includes an identification/authentication of the company, customer (name, address, license ID etc.) and the involved device (PSD manufacturer ID, PSD serial no., PSD model ID etc.) and should be logged in an appropriate way.

An intermediate step includes a verification of the customer/company data gathered during the preparatory step and the checking of the authorization for PIN reset operations. Then, the initial PIN is retrieved from the database, and the customer and/or his company are informed in an confidential way about the value of the initial PIN (e.g. by fax, registered mail or email). If verification cannot be accomplished the process is stopped.

As a final step, processes and data flows for PIN reset are shown below

The initial PIN used by the customer during the final step for authentication, should be changed as part of the PIN reset operation in a manner similar to the case when the PSD is used for the first time. However, this is not enforced technically but only recommended to the customer in a appropriate way (e.g. as part of process 3).

Customer ***Host*** ***PSD***

Process 0

Start of PIN reset procedure

<------------------------>

Process 1

1) Generates 64 random bits S

------------------------>

$M_0 = S$

Process 2

If PRO> PRO$_{max}$ device gets locked

1) Increments PRO (Reset operation counter)

2) Sets $PIN'_{ref} := PIN'_{init}$

3) Generates 64 random bits R

$M_1 = R$

<------------------------

Process 3

1) Prompts Customer for entry of *initial PIN* and new PIN

Run the PIN Modification Procedure here starting from Process 4 (see above)

------------------------------------ **End of *PIN Reset* Procedure** ------------------------------

As part of process 2 immediately above, the customer must be informed in a clear and unequivocal way about the remaining number of reset operations before the PSD is locked.

Referring to Fig. 4, and based on the above discussion, the various PIN states and values which exist are illustrated for PIN initialization, the first PIN verification, subsequent PIN verification, PIN modification, and PIN reset.

In accordance with the invention, there are a variety of ways in which the security of the PIN can be managed in addition to those disclosed above. Another possibility is for the customer, when ordering the PSD, to specify a customer chosen sequence of digits for which the customer takes responsibility. This may be some sequence of special significance to the customer, but as noted above, should be selected in accordance with common sense security guidelines. This customer selected PIN is then encoded and placed in the PSD in its encoded form as the original PIN used for shipping. As noted above, it should be changed when the PSD arrives at the customer.

There are two possibilities for what can be done in the situation where the customer supplies the PIN. In a first case, it can be treated in the same manner as a randomly generated PIN. Its value can be stored in database 36 (Fig. 1), and if the customer has difficulties and needs to obtain the PIN, the manufacturer can provide the data, as described above or using the procedure outlined below. However, for additional security, it is possible to erase all traces of the PIN value from the manufacturer's site; and in particular from server 34 and database 36. In principle, since it was the customer who provided the initial PIN, the customer should be able to furnish it in cases where it becomes necessary, without consulting with the manufacturer. In this case, once the PSD has been shipped to the customer, and all traces of it have been eliminated from the manufacturer's records, the manufacturer no longer has any security obligations whatsoever with respect to the PIN.

It will be recognized that even if the manufacturer supplies the initial PIN, as described above, it is possible for the manufacturer, after shipping the PSD to the customer and sending the PIN by a separate communication channel (which may be encrypted), to discard all traces of the PIN. However, this is a rather extreme case, perhaps reserved for situations in which very high levels of security need to be maintained. In this case, if the initial PIN is lost, it may not be possible to again access the PSD.

In a preferred embodiment for the PIN reset procedure, at the time the customer needs to recover the initial PIN of the PSD due to loss of the present PIN, the customer causes, via modern or internet connection between PSD host and provider or manufacturer data center, the PSD to remotely communicate with the data center for the purpose of providing the data center with knowledge secured via secret and/or public key authentication standards of private information relating to the PSD (e.g. device identification, authorization number, account number, or the like). Once the data center authenticates the PSD, the data center causes the initial PIN (archived in its server database) to be securely communicated to the requesting PSD. The PSD thereafter would have, in its PIN memory, the initial manufactured PIN, reintroduced. The customer would then be informed by an alternate method (email, FAX, telephone) of the initial PIN value. Thereafter, the customer would proceed to change the PIN to the user desired value. It will be recognized that this PIN reset procedure lends itself well to automation, so that the PIN in the PSD can be automatically reset to the original PIN upon an authorized request communicated by the user. As an additional security feature, a dedicated telephone number for a particular customer may be maintained.

It should be understood that the foregoing description is only illustrative of the invention. Various alternatives and modifications can be devised by those skilled in the art without departing from the invention. Accordingly, the present invention is intended to embrace all such alternatives, modifications and variances which fall within the scope of the appended claims.

CLAIMS

What is claimed is:

1. A method for generating a PIN, comprising:

generating a number of random binary bits;

determine the least significant bits of said number of bits;

converting the least significant bits to a decimal integer;

shifting the values of the integer by a predetermined constant to produce a shifted integer; and

encoding the shifted integer as bits in a PIN block in accordance with a standard.

2. The method of claim 1 wherein the standard is

ISO 9564-1.

3. The method of claim 1, wherein the number of random bits is sixty-four.

4. The method of claim 1, wherein the number of least significant bits is sixteen.

5. The method of claim 1, wherein the constant is 173845.

6. The method of claim 1 wherein the PIN block includes:

a control field;

a PIN length designation field;

a series of PIN digit field;

at least one PIN/transaction digit; and

a series of transaction digit fields.

7. The method of claim 6, wherein each PIN digit field represents a binary number having a decimal value of from zero to nine.

8. The method of claim 6, wherein the control field is the binary number 0001.

9. The method of claim 6, wherein the PIN length field contains a binary number having a decimal value of four, five or six.

10. The method of claim 6, wherein the at least one PIN/transaction digit is determined in accordance with PIN length.

11. The method of claim 6, wherein the transaction digit fields are each four bit binary fields representing a decimal digit of zero to nine.

12. The method of claim 1 wherein the generating of the number of random binary bits is done by using a pseudo random number generator.

13. A method for managing security of a PIN used to provide access to a secure device, comprising:

choosing the PIN;

storing an encrypted version of the PIN in the device; and communicating the PIN to a user of the device via a communication channel separate and apart from a channel used to provide the device to the user.

14. The method of claim 13, wherein said communication channel is a secure channel.

15. The method of claim 14, further comprising using encryption to render said communication channel secure.

16. The method of claim 13, wherein the user of said device chooses said PIN.

17. The method of claim 16, wherein a manufacturer of said device causes said encrypted version of said PIN to be stored in said device.

18. The method of claim 17, further comprising the manufacturer retaining a record of said PIN.

19. The method of claim 17, further comprising said manufacturer discarding all records of said PIN.

20. The method of claim 13 wherein said PIN is chosen using a random process.

21. The method of claim 20, wherein said PIN is chosen by:

generating a number of random binary bits;

determine the least significant bits of said number of bits;

converting the least significant bits to a decimal integer;

shifting the values of the integer by a predetermined constant to produce a shifted integer; and

encoding the shifted integer as bits in a PIN block in accordance with a standard.

22. The method of claim 21, wherein a manufacturer of said device causes said encrypted version of said PIN to be stored in said device.

23. The method of claim 22, further comprising the manufacturer retaining a record of said PIN.

24. The method of claim 22, further comprising said manufacturer discarding all records of said PIN.

25. The method of claim 13, wherein said device stores the value of funds.

26. The method of claim 13, wherein said device is a postal security device.

27. A method for resetting a PIN in a secure device comprising:

(a) sending a message to a data center having an original PIN for said device, said message including authorization data indicative of at least one of the device and an authorized user of said device, and

(b) securely communicating the original PIN to the location of the device.

28. The method of claim 27, wherein the device has a current PIN, further comprising replacing the current PIN with the original PIN.

29. The method of claim 27, wherein the communicating of the original PIN comprises:

sending the original PIN to the user of the device; and

the user of the device entering the original PIN into the device.

30. The method of claim 27 wherein at least one of (a) and (b) are performed using at least one of a secure communication channel and secure communication techniques.

ABSTRACT

A method for securely generating a PIN comprises generating a number of random binary bits; determining the least significant bits of the number of bits; converting the least significant bits to a decimal integer; shifting the value of the integer by a predetermined constant to produce a shifted integer; and encoding the shifted integer as bits in a PIN block in accordance with a standard. A method for managing security of a PIN used to provide access to a secure device comprising choosing the PIN; storing an encrypted version of the PIN in the device; and communicating the PIN to a user of the device via a communication channel separate and apart from a channel reset to provide the device to the user. A method for resetting a PIN in a secure device comprising sending a message to a data center having an original PIN for the device, the message including authorization data indicative of at least one of the device and an authorized user of the device, and securely communicating the original PIN to the location of the device.

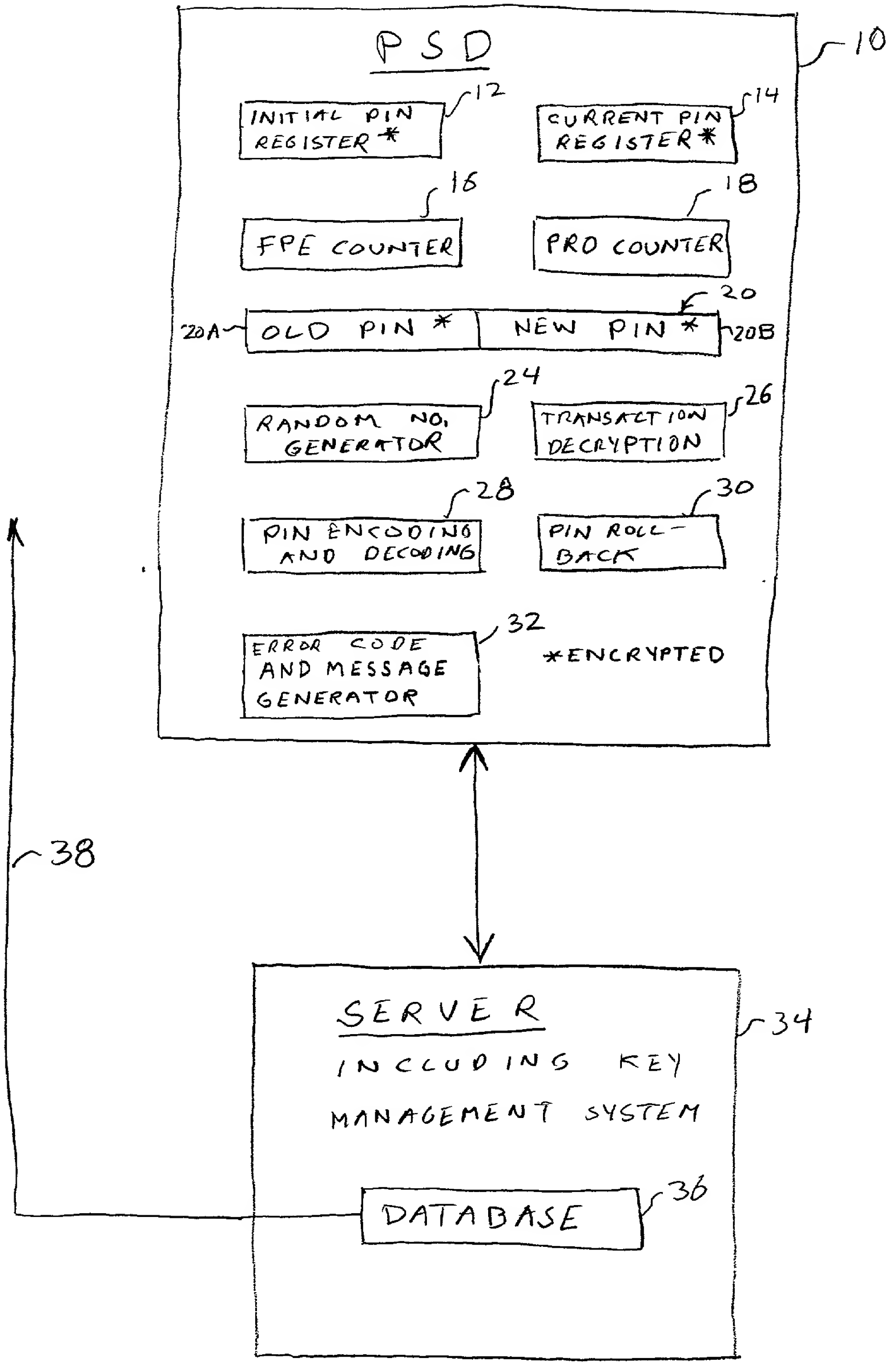
PSD
10
INITIAL PIN REGISTER *
12
CURRENT PIN REGISTER *
14
FPE COUNTER
16
PRO COUNTER
18
20
20A
OLD PIN *
NEW PIN *
20B
RANDOM NO. GENERATOR
24
TRANSACTION DECRYPTION
26
PIN ENCODING AND DECODING
28
PIN ROLL-BACK
30
ERROR CODE AND MESSAGE GENERATOR
32
*ENCRYPTED
38
SERVER
INCLUDING KEY MANAGEMENT SYSTEM
34
DATABASE
36

Fig. 1

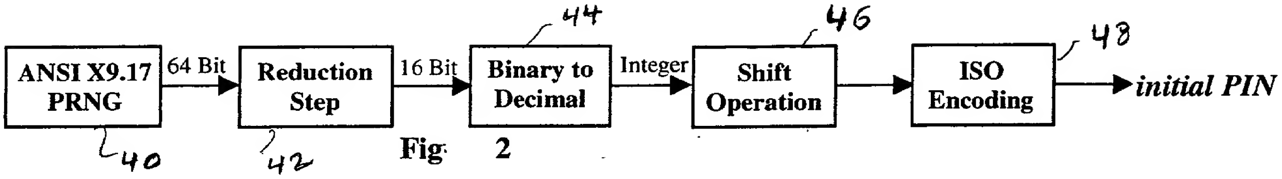

Fig 2

50

Bit no.	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
	C	N	P	P	P	P	P/T	P/T	T	T	T	T	T	T	T	T
	52	54	56	58	60	62	64	66	68	70	72	74	76	78	80	82

Where :

C = Control field	4-bit binary number 0001
N = PIN length	4-bit binary number with permissible values 0100 (4) to 0110 (6)
P = PIN digit	4-bit field with permissible values 0000 (zero) to 1001 (9)
P/T = PIN/ Transaction digit	Determined by PIN length
T = Transaction digit	4-bit binary number 0000

Fig. 3

	Start of Process		End of Process	
PIN Initialization			Status	Value
PIN_{init} :			*active*	*initial PIN*
PIN_{cust} :			*non-active*	*initial PIN*
1st PIN Verification	Status	Value	Status	Value
PIN_{init} :	*active*	*initial PIN*	*non-active*	*initial PIN*
PIN_{cust} :	*non-active*	*initial PIN*	*active*	*initial PIN*
PIN Verification	Status	Value	Status	Value
PIN_{init} :	*non-active*	*initial PIN*	*non-active*	*initial PIN*
PIN_{cust} :	*active*	*Customer PIN*	*active*	*Customer PIN*
PIN Modification	Status	Value	Status	Value
PIN_{init} :	*non-active*	*initial PIN*	*non-active*	*initial PIN*
PIN_{cust} :	*active*	*Customer PIN*	*active*	*new Customer PIN*
PIN Reset	Status	Value	Status	Value
PIN_{init} :	*non-active*	*initial PIN*	*active*	*initial PIN*
PIN_{cust} :	*active*	*Customer PIN*	*non-active*	*Customer PIN*

Fig. 4